徐彥旻(b03901027)

蕭旭君教授

密碼學與資訊安全

2017 年 3 月 15 日

Reading Critique #3

http://thehackernews.com/2017/03/android-adware-malware-google.html

Summary

Google 工程師在例行的廣告品質評估中發覺可疑的廣告流量，因而發現了一系列在 Google 官方應用程式商店的 PHA （潛在有害的應用程式）。

這樣的應用程式可以濫用權限，以搜集敏感的個資、利用彈出廣告轟炸使用者、在背景安裝別的應用，以及寄簡訊啟用付費服務等等。這系列的應用程式被稱為「Chamois」(法語中的羚羊之意)。

Chamois 來自於巨大的開發者網絡，雖然 Google 已經用驗證程式阻擋了 Chamois ，並且禁止了一些想要用 Google 廣告系統賺錢的人，但其安全團隊仍需要費勁研究大量的看起來是專業開發者所寫的程式碼，以釐清跟 Chamois 相關的應用程式到底有多少。

Reflection

在這個新聞中，Google 廣告系統的可用性、以及使用者手機的保密性、完整性與可用性遭到攻擊

在此的風險模型會是：攻擊者是一群人的網絡，有專業的程式能力，可以將惡意程式包在其他的應用當中，並且還可以有許多的階段，以避免偵測。在可以賺錢的引誘之下，想要「玩」Google 廣告系統的人應該是不會少的。

http://thehackernews.com/2017/03/android-malware-apps.html

Summary

至少三十六支高規格的手機被發現在韌體層級上有預先裝好的惡意程式，這些惡意程式分成兩個系列， Loki 與 SLocker。 Loki 可以取得最高權限，並且監看使用者的活動，取得聯絡人、通話紀錄、位置等資料。 SLocker 則是勒索程式。

這些惡意程式在手機生產鏈的某處被裝載，一至於使用者以為自己拿到的是全新的手機時，其實裡頭已經被動過手腳了，必須要刷機或是用相當複雜的方式才能去除。

Reflection

在這個新聞中，使用者的的保密性、完整性與可用性都遭受威脅。

安全是必須要顧到最弱的環節的——甚至在生產鏈上就必須要做好相關的規劃，否則其他部分做的再好，惡意軟體還是拿得到最高權限，並且，這樣子的事件不僅僅是安全議題，也造成生產商的形象損害，背負品管不良的惡名。